Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Kyung H. Shin** **Group Art Unit 2143**	Facsimile No.: **571/273-8300**
From: Jennifer Pilcher Legal Assistant to Wayne Bailey	No. of Pages Including Cover Sheet: **28**

Message:

Enclosed herewith:

- Transmittal of Appeal Brief; and
- Appeal Brief.

Re: Application No. **09/692,348**
Attorney Docket No: **AUS9-2000-0631-US1**

Date: Thursday, April 13, 2006

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Beukema et al.**

Serial No.: **09/692,348**

Filed: **October 19, 2000**

For: **Method and Apparatus for Reporting Unauthorized Attempts to Access Nodes in a Network Computing System**

Group Art Unit: **2143**

Examiner: **Shin, Kyung H.**

Attorney Docket No.: **AUS9-2000-0631-US1**

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on April 13, 2006.

By: _____
Jennifer Pilcher

TRANSMITTAL OF APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37)

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEY FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER

APR 13 2006

Docket No. AUS9-2000-0631-US1 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Beukema et al.**

Serial No. **09/692,348**

Filed: **October 19, 2000**

For: **Method and Apparatus for Reporting Unauthorized Attempts to Access Nodes in a Network Computing System**

Group Art Unit: **2143**

Examiner: **Shin, Kyung H.**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on April 13, 2006.

By: Jennifer Pilcher

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on February 17, 2006.

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

04/14/2006 EAYALEW1 00000053 090447 09692348

01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, N.Y.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-25

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-25
4. Claims allowed: none
5. Claims rejected: 1-25
6. Claims objected to: none

C. CLAIMS ON APPEAL

The claims on appeal are: 1-25

STATUS OF AMENDMENTS

No amendment after final rejection was filed for this case.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

A system area network (SAN) provides an ability to partition the use of various components within the network, where some devices may be private to a given node, while others are shared between multiple nodes in the network. In some cases, a node may try to access other nodes without authorization. In other cases, the access may be a malicious attempt by a node to access nodes within a network outside the domain of access for that given node. Claim 1 is directed to a method for handling unauthorized attempts to access a node.

Specifically, Claim 1 is directed to a method in a node for managing attempts to access the node. The node receives a packet from a source, where the packet includes a first key. This first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node receiving the packet can determine which of the partitions of the multi-partitioned network can access the node receiving the packet. The node determines whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node. If the first key does not match the second key, the packet is dropped by the node without a response to the source of the packet. In addition, the node stores information about the packet and sends such information to a selected recipient in response to a selected event. The above node access methodology is described in the Specification at page 23, line 1 – page 30, line 1 with reference to Figures 6-8 and with particular reference to Figure 8, elements 800-820.

Such multi-partitioning network advantageously provides an ability to segregate and selectively share devices, where some devices are private to a given node and others are shared between nodes (Specification page 23, lines 1-4). The claimed partition key advantageously provides an ability to determine which partitions can access a given node, as well as enable such segregation and selective sharing of devices in the multi-partitioning network.

B. CLAIM 10 - INDEPENDENT

Claim 10 is directed to a method in a node for reporting access violations. A packet is received from a source, where the packet includes authentication information that is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is

used such that the node can determine which of the partitions of the multi-partitioned network can access the node. The received authentication information is verified to determine if the packet is from a partition authorized to access the node. If the received authentication information is unverified, the packet is dropped without a response to the source. Information from the packet is stored, and sent to a selected recipient in response to a selected event.

The above access violation methodology is described in the Specification at page 23, line 1 – page 30, line 1 with reference to Figures 6-8 and with particular reference to Figure 8, elements 800-820.

C. CLAIM 12 - INDEPENDENT

Claim 12 is directed to a data processing system comprising a bus system, a channel adapter unit connected to a system area network fabric, a memory connected to the bus system, wherein the memory includes as set of instructions; and a processing unit connected to the bus system. The processing unit executes the set of instructions to (i) receive a packet from a source, where the packet includes a first key that is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node; (ii) determine whether the first key matches a second key for the node; (iii) drop the packet without a response to the source if the first key does not match the second key; (iv) store information from the packet; and (v) send the information to a selected recipient in response to a selected event.

The above node access methodology and data processing system is described in the Specification at page 10, lines 9 – 17 and page 23, line 1 – page 30, line 1 with reference to Figures 1 and 6-8 and with particular reference to Figure 1, elements 102, 118, 120, 126, 128, 130, 132 and 134 and Figure 8, elements 800-820.

D. CLAIM 13 - INDEPENDENT

Claim 13 is directed to a node comprising a receiving means (e.g. Figure 1, HCA elements 118, 120 and TCA elements 158-166 and 172) for receiving a packet from a source, where the packet includes a first key that is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can

determine which of the partitions of the multi-partitioned network can access the network node. The node also comprises a determining means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node, a dropping means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for dropping the packet without a response to the source if the first key does not match the second key, a storing means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for storing information from the packet; and a sending means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for sending the information to a selected recipient in response to a selected event.

The above node is described in the Specification at page 8, lines 1-11, page 26, lines 7-10 and page 23, line 1 – page 30, line 1 with reference to Figures 1 and 6-8 and with particular reference to Figure 1, elements 102 – 124, 158-166 and 172 and Figure 8, elements 800-820.

E. CLAIM 22 - INDEPENDENT

Claim 22 is directed to a node comprising a receiving means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for receiving a packet from a source, where the packet includes authentication information that is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node. The node also comprises a verifying means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for verifying the received authentication information to determine if the packet is from a partition authorized to access the node, a dropping means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for dropping the packet without a response to the source if the received authentication information is unverified, a storing means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for storing information from the packet, and a sending means (e.g. Figure 1, HCA elements118, 120 and TCA elements 158-166 and 172) for sending the information to a selected recipient in response to a selected event.

The above node is described in the Specification at page 8, lines 1-11, page 26, lines 7-10 and page 23, line 1 – page 30, line 1 with reference to Figures 1 and 6-8 and with particular reference to Figure 1, elements 102 – 124, 158-166 and 172 and Figure 8, elements 800-820.

F. CLAIM 24 - INDEPENDENT

Claim 24 is directed to a computer program product in a computer readable medium for use in a node for managing attempts to access the node, the computer program product comprising instructions for executing the steps recited in Claim 1. The explanation of the subject matter described with respect to Claim 1 above is hereby incorporated by reference.

G. CLAIM 25 - INDEPENDENT

Claim 25 is directed to a computer program product in a computer readable medium for use in a node for reporting access violations, the computer program product comprising instructions for executing the steps recited in Claim 10. The explanation of the subject matter described with respect to Claim 10 above is hereby incorporated by reference.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-4, 7-16 and 19-25)

Claims 1-4, 7-16 and 19-25 stand rejected under 35 U.S.C. § 103 as being unpatentable over Williams et al. (US Patent No. 6,304,973) in view of Frezza et al. (US Patent No. 4,638,356) and further in view of Moiin et al. (US Patent No. 6,449,641).

B. GROUND OF REJECTION 2 (Claims 5, 6, 17 and 18)

Claims 5, 6, 17 and 18 stand rejected under 35 U.S.C. § 103 as being unpatentable over Williams et al. (US Patent No. 6,304,973) in view of Frezza et al. (US Patent No. 4,638,356) and further in view of Moiin et al. (US Patent No. 6,449,641) and further in view of Kekic et al. (US Patent No. 6,664,978).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-4, 7-16 and 19-25)

A.1. Claims 1-4

Appellants initially show error in the rejection of Claim 1 in that the Examiner has mischaracterized the teachings of the cited Frezza reference. Claim 1 recites a step of "receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node". As can be seen, the received packet includes a partition key, and this partition key is used such that the node (which received the packet) can determine which of the partitions of the multi-partitioned network can access the node (which received the packet). In rejecting this aspect of Claim 1, the Examiner cites Frezza's teaching at col. 6, lines 37-44 as teaching this claimed step. Appellants urge that to the contrary, this Frezza passage teaches a subscriber node that receives an encrypted channel access code (CAC). The encrypted CAC is decrypted using an internal decryption key, and this decrypted channel access code is then used by the subscriber node to generate frame verifier codes which are subsequently used by such subscriber node when placing transmitting packets on the network (Frezza col. 6, lines 37-44; col. 4, lines 1-24). This received channel access code is not associated with a particular partition of a multi-partitioned network, and is not used by the receiving node to determine which partitions can access such node, but is instead used to subsequently generate frame verifiers that are included in data packets that are unconditionally placed on the network.

Appellants further show that the secret node key as described by Frezza (col. 2, lines 42-44; col. 6, lines 38-39) also does not teach or suggest the claimed partition key – for numerous reasons. First, this secret node key is internally maintained within a subscriber node (see Figure 1, element 40), and is not part of any type of communication packet that is received. Claim 1 expressly recites receiving, by the node, a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key. Frezza's secret key is internally maintained since it is a decryption key used to decrypt received packets. If it were to be somehow placed on the network (such that is could be received by a node, as per Claim 1), the entire security system

would be compromised as anyone on the network could access this secret node decryption key – and thus it would no longer be a secret key. The fact that this secret key is internally maintained within a node can also be seen by viewing the content of a packet sent on the network, as shown in Frezza's Figure 5. This packet, which is what is transmitted on the network (Frezza col. 4, lines 25-35), does not include Frezza's secret node key, further evidencing that Frezza's secret node key is not included in a packet that is received by a node (as required by the features of Claim 1). Thus, Claim 1 is further shown to not be obvious in view of the cited references, and there are missing claimed features not taught or suggested by the cited references.

Still further, this secret node key is not used such that *a node receiving a key* can determine *which of the partitions* of the multi-partitioned network *can access the node.* Rather, this internal key is used to decrypt a received, encrypted, channel-access code which is then used by the subscriber node to generate frame verifier codes. These generated frame verifier codes are then transmitted by the subscriber node, and another node (the distributed access controller (Figure 1, element 28; col. 6, lines 45-58) monitors these codes to ensure they match the codes internally maintained within a look-up table. If they do not match, the channel is jammed by the distributed access controller (Frezza col. 7, lines 7-17). Claim 1 expressly recites that the partition key is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node receiving the packet can determine which of the partitions of the multi-partitioned network can access the node receiving the packet. Frezza's secret node key does not provide any such functionality, and thus Claim 1 is further shown to not be obvious in view of the cited references, and there are missing claimed features not taught or suggested by the cited references.

Still further with respect to Claim 1, Appellants urge that none of the cited references teach or suggest that the *node that actually receives a packet containing a partition key - itself* - determines whether the received packet is from a partition authorized to access the node (that receives a packet containing the partition key). In effect, the partition key receiving node is policing attempted accesses to itself by other nodes. The cited Frezza reference – which is being used as teaching the claimed step of receiving a partition key - teaches (1) a subscriber node that receives an encrypted key which is decrypted by such node and then used by such node to generate frame verifiers which are then used by such node during subsequent, and unconditional, transmission of data packets onto the network, and (2) a digital access controller which matches

received frame verifier codes transmitted by such subscriber node with internally maintained codes and transmits a jamming signal on the channel if such codes do not match. The subscriber node in this scenario (2) is not attempting to access the digital access controller, but instead is attempting to access a different, head-end node, and this digital access controller is intentionally separated from the head-end node for which access is sought, in order to provide decentralized control of the network (col. 1, lines 19-61). Thus, there is no teaching of a node receiving a packet having a partition key and *determining whether the received packet is from a partition authorized to access the node that received the packet*.

It has thus been shown that it is unreasonable to interpret Frezza's secret node key to be the claimed partition key, as it is (1) not received by a node, but internally maintained within a node and kept secret within the node, (2) is not used to determine, by the node receiving a partition key, *which of the partitions* of the multi-partitioned network *can access the node* that received the key, and (3) the node which processes this secret node key – the subscriber node – is the node actually *seeking access* to network resources, and not *determining access* authorization.

Appellants have thus shown that there are missing claimed features not taught/suggested by the cited references – including the claimed partition key and associated processing with respect to such partition key – and thus Claim 1 has been erroneously rejected under 35 U.S.C. § 103.

A.2. Claims 7 and 19

Applicants initially show error in the rejection of Claim 7 for reasons given above with respect to Claim 1 (of which Claim 7 depends upon).

Further with respect to Claim 7, it is urged that none of the cited references teach or suggest the claimed feature of "wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network". As can be seen, the node which receives the packet having the partition key includes both a private device and a shared device. In rejecting Claim 7, the Examiner cites Williams' teaching at col. 27, lines 38-47 and Moiin's teaching at col. 4, lines 15-19; col. 4, line 66 – col. 5, line 4; col. 13, lines 41-44; and col. 13, lines 52-55 as teaching this claimed feature. Applicants show that the cited Williams passage at col. 27, lines 38-47 states:

> "The foregoing descriptions and drawings should be considered as illustrative only of the principles of the invention. The invention may be configured in a variety of manners and is not limited by the design of the preferred embodiment. Numerous applications of the present invention will readily occur to those skilled in the art. Therefore, it is not desired to limit the invention to the specific examples disclosed or the exact construction and operation shown and described. Rather, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention."

As can be seen, this passage makes no mention whatsoever of any of the specific features recited in Claim 7, such as the device that is private to a node and another device that is shared with a partition of a multi-partitioned network. Nor do the teachings of the cited Moiin passages overcome this teaching deficiency. Moiin states at col. 4, lines 15-19; col. 4, line 66 – col. 5, line 4; col. 13, lines 41-44; and col. 13, lines 52-55:

> In accordance with the present invention, cluster membership in a distributed computer system is determined by determining with which other nodes each node is in communication and distributing that connectivity information through the nodes of the system (col. 4, lines 15-19).
>
> With the failures described above, the cluster membership can be partitioned into two or more fully-connected subsets of nodes having a majority of the votes, a minority of the votes, or exactly half of the votes. The first two cases may be resolved by only allowing a subset having a majority vote to form the next generation of the cluster (col. 4, line 66 – col. 5, line 4).
>
> In the case of a shared disk configuration with CVM and Netdisk, it is assumed that **the master and its backup node for all NetDisk devices have direct physical access to the underlying physical device** (col. 13, lines 41-44) (emphasis added by Applicants).

> We also assume that information about the primary and backup ownership of a NetDisk device or other resources is maintained in the Cluster Configuration Database, CCD, and is **available to all nodes** in a consistent manner (col. 13, lines 52-55) (emphasis added by Applicants).

As can be seen, none of these cited passages teach a node that receives a partition key includes two devices, where one of the devices is private to the node and the other is shared. For example, all physical devices are connected to each of two nodes (Moiin Figure 2), and certain information pertaining to all of the physical devices is available to all of the nodes - and thus they are not private to a given node. Restated, Moiin teaches the clustering of nodes, and all devices for a given node are treated the same with respect to other nodes (col. 2, lines 16-54). Thus, there is no teaching or suggestion of a node that receives a partition key includes two devices, where one of the devices is private to the node and the other is shared. It is thus further shown that Claim 7 has been erroneously rejected under 35 U.S.C. § 103, as there are additional claimed features not taught or suggested by any of the cited references.

A.3. Claims 9 and 21

Applicants initially show error in the rejection of Claim 9 for reasons given above with respect to Claim 1 (of which Claim 9 ultimately depends upon).

Applicants further show error in the rejection of Claim 9 for reasons given above with respect to Claim 7 (of which Claim 9 depends upon).

Still further with respect to Claim 9, such claim has been erroneously rejected as none of the cited references teach or suggest the claimed feature of "wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet". As can be seen, the selected recipient – which has had information sent to it in response to a selected event, per Claim 1 – is a subnet manager attached to a subnet. In rejecting Claim 9, the Examiner states that this claimed feature is taught by Williams at col. 17, lines 19-27 and col. 27, lines 38-47. The Williams passage at col. 27 has already been reproduced above, and it is urged that this passage makes no mention whatsoever of

any of the specific features recited in Claim 9, such as a subnet manager. As to the passage cited at col. 17, there Williams states:

> "The network 10 provides selectable auditing of the following types of events: login and logout of security officers at the NSC; change of security databases at the NSC; I&A of principals; statistical events, providing detailed information about the individual packets transmitted and received; exception events, including attempts to violate the security window, send to or receive from an unauthorized association, etc.; TCP/UDP port filtering rejections; and, TCP opens and closes."

As can be seen, there is no mention of any type of subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet. Rather, this passage describes an internal audit function (which merely audits the occurrence of activities that occur). Claim 9 specifically requires that the selected recipient – *which has had information sent to it in response to a selected event*, per Claim 1 – is a subnet manager attached to a subnet. It is thus further shown that Claim 9 has been erroneously rejected, as there are additional missing claimed features not taught or suggested by any of the cited references.

B. GROUND OF REJECTION 2 (Claims 5, 6, 17 and 18)

B.1. Claims 5, 6, 17 and 18

Applicants show that Claim 5 (in combination with independent Claim 1) recites "receiving, by the node, a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node receiving the packet can determine which of the partitions of the multi-partitioned network can access the node receiving the packet". Neither Williams, Frezza, Moiin nor Kekic teach or suggest a partition key that is used such that the node receiving the packet can determine which of the partitions of the multi-partitioned network can access the node receiving the packet, for substantially the same reasons as those given above with respect to Claim 1. Thus, it is urged that Claim 5 is not obvious in view of the combination of the cited Williams-Frezza-Moiin references in combination with the

additionally cited Kekic reference, as there are missing claimed features not taught or suggested by any of such cited references. Therefore, Claim 5 has been erroneously rejected under 35 U.S.C. § 103.

Still further with respect to Claim 5, and contrary to the Examiner's assertion, the cited Kekic reference does not teach incrementing a counter when a key mismatch is encountered. For example, the cited passage at Kekic col. 27, lines 12-18 states (the entire paragraph is being reproduced herewith to give the proper context):

> In one embodiment, as described above, the event management model is a set of rules associated with a managed computer network element which causes specified actions to take place when a specified criterion is satisfied. A rule is evaluated upon occurrence of a predefined polling event or trap event for the managed computer network element. A typical criterion is testing whether a network management variable value has exceeded some threshold value. The specified actions can include, for example changing a component's state, executing a server operating system command, forwarding a trap to another host, and/or logging pertinent information. The severity associated with a element component's state is visually highlighted in the visual display of the managed element, and a visual cue notifies the user whenever information is logged. By carefully defining the polling and trap events and the set of rules, an accurate picture is constructed of extraordinary element behavior and advanced problem analysis is automatically performed to aid in common network management strategies including configuration management, fault management, and performance management.

As can be seen, there is no mention of any type of key or key mismatch determination, or the incrementing of a counter upon occurrence of a key mismatch. Rather, this passage teaches that the events are either (i) a predefined polling event, or (ii) a trap event. Thus, Claim 5 has been

erroneously rejected as a proper prima facie showing of obviousness has not been established by the Examiner[1].

In conclusion, Appellants have shown numerous errors in the Examiner's final rejection of all claims in the present case, and Appellants thus request that the Board reverse such final rejection.

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

[1] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id. To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a node for managing attempts to access the node, the method comprising:

receiving, by the node, a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node receiving the packet can determine which of the partitions of the multi-partitioned network can access the node receiving the packet;

determining, by the node, whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node;

dropping, by the node, the packet without a response to the source of the packet if the first key does not match the second key;

storing, by the node, information from the packet; and

sending, by the node, the information to a selected recipient in response to a selected event.

2. The method of claim 1, wherein the selected event is a request from the recipient for the information.

3. The method of claim 1, wherein the selected event is an occurrence of a trap.

4. The method of claim 1, wherein the selected event is a periodic event.

5. The method of claim 1 further comprising:

incrementing a counter source if the first key does not match the second key.

6. The method of claim 5, wherein the selected event occurs when the counter exceeds a threshold value.

7. The method of claim 1, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

8. The method of claim 1, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

9. The method of claim 7, wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet.

10. A method in a node for reporting access violations, the method comprising:

receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node that received the packet can determine which of the partitions of the multi-partitioned network can access the node that received the packet;

verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

dropping the packet without a response to the source if the received authentication information is unverified;

storing information from the packet; and

sending the information to a selected recipient in response to a selected event.

11. The method of claim 10, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

12. A data processing system comprising:

a bus system;

a channel adapter unit connected to a system area network fabric;

a memory connected to the bus system, wherein the memory includes as set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the data processing system can determine which of the partitions of the multi-partitioned network can access the data processing system; determine whether the first key matches a second key for the data processing system; drop the packet without a response to the source if the first key does not match the second key; store information from the packet; and send the information to a selected recipient in response to a selected event.

13. A node comprising:

receiving means for receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node;

determining means for determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node;

dropping means for dropping the packet without a response to the source if the first key does not match the second key;

storing means for storing information from the packet; and

sending means for sending the information to a selected recipient in response to a selected event.

14. The node of claim 13, wherein the selected event is a request from the recipient for the information.

15. The node of claim 13, wherein the selected event is an occurrence of a trap.

16. The node of claim 13, wherein the selected event is a periodic event.

17. The node of claim 13 further comprising:

incrementing means for incrementing a counter source if the first key does not match the second key.

18. The node of claim 17, wherein the selected event occurs when the counter source exceeds a threshold value.

19. The node of claim 13, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network.

20. The node of claim 13, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address.

21. The node of claim 19, wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet.

22. A node comprising:

receiving means for receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

verifying means for verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

dropping means for dropping the packet without a response to the source if the received authentication information is unverified;

storing means for storing information from the packet; and

sending means for sending the information to a selected recipient in response to a selected event.

23. The node of claim 22, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network .

24. A computer program product in a computer readable medium for use in a node for managing attempts to access the node, the computer program product comprising:

first instructions for receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the network node;

second instructions for determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node;

third instructions for dropping the packet without a response to the source if the first key does not match the second key;

fourth instructions for storing information from the packet; and

fifth instructions for sending the information to a selected recipient in response to a selected event.

25. A computer program product in a computer readable medium for use in a node for reporting access violations, the computer program product comprising:

first instructions for receiving a packet from a source, wherein the packet includes authentication information, wherein the authentication information is associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node;

second instructions for verifying the received authentication information to determine if the packet is from a partition authorized to access the node;

third instructions for dropping the packet without a response to the source if the received authentication information is unverified;

fourth instructions for storing information from the packet; and

fifth instructions for sending the information to a selected recipient in response to a selected event.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.